UNITED STATES DISTRICT COURT

for the
Eastern District of Pennsylvania

In the Matter of the Search of The Cellular Telephone described as a black in color, Apple iPhone, AT&T Mobile Cellular Telephone, with telephone number 484-274-9937	)	Magistrate No. 22-mj-444

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

located in the Eastern District of Pennsylvania, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 922(g)(5)(A)&(B), 18 U.S.C. §924(a)(1)(A)	Unlawful for any person unlawfully in the US to possess in or affecting commerce, any firearm or ammunition; and it is unlawful to knowingly make any false statement or representation with respect to information required to be kept in the records of a federal firearms licensee.

The application is based on these facts:

See Affidavit in Support of Application for Search Warrant.

- ☐ Continued on the attached sheet
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Carmen Dvorak de Morales

Applicant's signature

Carmen Dvorak de Morales, SA, FBI

Printed name and title

Sworn to before me and signed in my presence:

Date: March 18, 2022 4:11 pm /s/ Richard A. Lloret

Judge's signature

City and state: Philadelphia, PA

Honorable Richard A. Lloret, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF: THE CELLULAR TELEPHONE DESCRIBED AS BLACK IN COLOR, APPLE iPHONE, AT&T MOBILE CELLULAR TELEPHONE, WITH TELEPHONE NUMBER 484-274-9937	Magistrate No. 22-mj-444

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

INTRODUCTION AND AGENT BACKGROUND

1. I, Carmen Dvorak de Morales, am a Special Agent ("SA") with the Federal Bureau of Investigation, Philadelphia Division, Allentown Resident Agency. As such, I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, execute warrants issued under the authority of the United States and to make arrests for, offenses enumerated in Title 21, and Title 18, United States Code.

2. I am a Special Agent with the Federal Bureau of Investigation. I have been employed by the FBI since October 27, 2019, and, as such, I am a federal law enforcement officer within the meaning of Fed. R. Crim. P. 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request such a warrant. I am currently assigned to the Allentown Resident Agency ("ARA") of the Philadelphia Division. Prior to joining the FBI, I was employed as an Assistant State's Attorney with the Cook County State's Attorney's Office in Illinois from approximately December 2013 to October 2019. As a Special Agent, I have received instruction and on the job training in various aspects of law enforcement. During my employment with the FBI, I have participated in

investigations involving international and domestic terrorism, bank robberies, drug trafficking, financial institution fraud, human trafficking, and other federal violations. In the course of those investigations, I have employed the use of electronic surveillance techniques, have executed numerous search and arrest warrants, conducted physical and electronic surveillance, utilized information from cellular service providers, including historical cell site and location information, and secured other relevant information utilizing additional investigative techniques. Based on my participation in these debriefings and investigations, I am aware that individuals involved in committing these types of criminal acts commonly carry cellular telephones to and from their commission of the crimes and often use cellular telephones and other electronic devices in furtherance of their criminal activities. I am further aware that ninety six percent of American adults possess a cellular phone, and the substantial majority (eighty-one percent) possess a "smartphone."[1] .

3. Based on my training and experience and the training and experience of other agents, I am aware that data stored on electronic devices can remain for a long time. Furthermore, I am also aware that newer phones can store and contain data from several years ago; for instance, if an individual uses a social media or messaging application it can store data from several years ago (such as Facebook messenger, Whatsapp, or Tango). In addition, I am aware that some data, such as contacts, photographs, and text messages, can be transferred from old phones to new phones, either manually or by transferring a SIM card device that has the data on it. It is therefore reasonable to believe that the phone recovered during the investigation discussed below may have data stored from the user's interactions with co-conspirators during the course of the charged conspiracy, or may have older communications from social media sites stored on the phone.

4. Based on my training and experience, I know that those involved in illicit activities commonly utilize their cellular telephones to communicate with co-conspirators to facilitate, plan, and execute their illegal activities. For example, I know that these individuals often store contacts lists, address books, calendars, photographs, videos, and audio files, text messages, call logs, and voice mails in their electronic devices, such as cellular telephones, to be used in furtherance of their illegal activities.

5. Specifically, I know that those involved in illegal activities communicate with associates using cellular telephones to make telephone calls. If they are unable to reach the party called, they frequently leave voice mail messages. I am aware that Apple-based and Android-based phones download voice mail messages and store them on the phone itself so that there is no need for the user to call into a number at a remote location and listen to the message. In addition, I know those involved in illegal activities communicate with associates using cellular telephones and tablets to send e-mails and text messages. I know they also communicate with associates via social media networking sites and through messaging options via social media (e.g., Facebook messaging), or through other communication applications available to download and use on phones, including, but not limited to, "Whatsapp," "Signal," and "Telegram." By analyzing call and text/application communications, including any social media "chats" or messaging application communications, I may be able to determine others who have communicated with the defendant about the possible purchase of firearms.

6. Furthermore, cellular telephones also contain address books with names, addresses, photographs, and phone numbers of a person's regular contacts. In addition, I know that those involved with illicit activities often take photographs or make videos of themselves and others and retain them on their electronic devices such as cellular telephones. I am also

aware that individuals involved in illicit activities often take photographs or make videos of the proceeds of their illicit activities with their cellular telephones and tablets. Based on my training and experience, those who commit these crimes often store these items on their phones in order to show to associates, and/or to upload to social media.

7. Furthermore, based on my training and experience and the training and experience of other agents, I know that individuals often use a cellular phone's Internet browser for web browsing activity related to their illicit activities. In addition, I know that these individuals also use their cellular telephone's Internet browser to update their social networking sites in order to communicate with others, locate possible sellers, and to post photographs of locations where they have traveled or purchases they have made in furtherance of their criminal activities.

8. In addition, individuals engaged in illicit activities sometimes use cellular telephones as navigation devices, obtaining maps and directions to various locations in furtherance of their criminal activities. These electronic devices may also contain GPS navigation capabilities and related stored information that could identify where these devices were located.

9. Furthermore, based on my training and experience, forensic evidence recovered from the review of a cellular telephone can also assist in establishing the identity of the user of the device, how the device was used, the purpose of its use, and when it was used. In particular, I am aware that cellular telephones are all identifiable by unique numbers on each phone, including: serial numbers, international mobile equipment identification numbers ("IMEI") and/or electronic serial numbers ("ESN"). In addition, I am aware that by using forensic tools, information/data that users have deleted may still be able to be recovered from the device.

10. I make this affidavit in support of an application for a search warrant of the

following mobile cellular telephone, as described in Attachment A: One (1) Apple iPhone AT&T Mobile Cellular Telephone bearing telephone number 484-274-9937 ("SUBJECT PHONE"), seized from the person of the defendant Mahmoud Ali Ahmad Rashwan ("the defendant") at the time of his arrest on March 12, 2022, which has been in the custody of the FBI ARA since the defendant's arrest.

11. This application seeks authority to search for and seize evidence, and fruit and instrumentalities of crimes against the United States, specifically in violation of Title 18, United States Code, Sections 922(g)(5)(A)&(B)[1], and 924(a)(1)(A)41(a)(1),[2] as described in Attachment B.

ELECTRONIC DEVICES

12. As described in Attachment B, this application seeks permission to search and seize evidence contained in the SUBJECT PHONE, in whatever form it is stored. As used herein, the term "electronic device" includes any electronic system or device capable of storing or processing data in digital form, in this case referring specifically to wireless or cellular telephone.

13. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices. In particular, I know that

[1] Title 18, United States Code, Section 922(g)((5) states: "it shall be unlawful for any person…who, being an alien (A) is illegally or unlawfully in the United States; or (B) has been admitted to the United States under a nonimmigrant visa … to possess in or affecting commerce, any firearm or ammunition.

[2] Title 18, United States Code, Section 924(a)(1)(A) makes it a crime for any individual to knowingly make any false statement or representation with respect to information required to be kept in the records of a federal firearms licensee. A Firearms Transaction Record, Form 4473, is information that is required to be kept in the records of a federal firearms licensee. Federal Firearm Licensees are required to maintain a record, in the form of a completed Form 4473, of the identity of the actual buyer of the firearms sold by the FFL holder, to ensure that the person was not prohibiting from purchasing a firearm.

electronic devices are likely to be repositories of evidence of crimes. I know that an electronic device such as a cellular telephone may contain data that is evidence of how the electronic device was used, data that was sent and received, and other records that may indicate the nature of the offense.

14. Furthermore, I know that electronic devices, such as cellular telephones, can store information for long periods of time. Examples of such information include text and multimedia message conversations, call history, voice mail messages, e-mails, photographs, and other data stored on the device. Similarly, I know from my training and experience that when cellular telephones are used to access the internet, a browser history is also frequently stored for some period of time on the electronic device. This information can sometimes be recovered with forensic tools.

15. Based on my experience and training, as well as the experience and training of other agents, I know that even when a user deletes information from a device, it can sometimes be recovered with forensics tools. Further, based on my experience and training, I know that other than the conventional mechanical hard drives that are traditionally in computers, becoming more prevalent are flash memory-based hard drives and devices. This technology has been traditionally used for small thumb drives where files and data are stored electronically, but has since evolved and is being used in computer hard drives known as "solid state hard drives" or SSD's and also being used in cell phones and smart phones. These devices do not operate like mechanical hard drives when it comes to how files and data are stored and deleted. These devices can move data around on the drive to maximize storage space and longevity of the drive, compress data, and may use different deletion techniques for how a deleted file is handled and

overwritten. The manner in which these devices function may limit how much data, if any, can be recovered from these types of devices.

16. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that searching electronic devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of electronic devices and software programs in use today that specialized equipment is sometimes necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of electronic devices, operating systems, or software applications that are being searched.

17. Furthermore, I am aware that electronic data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching electronic devices can require the use of precise, scientific procedures that are designed to maintain the integrity of electronic data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on electronic devices.

18. Also, I know from my training and experience that the volume of data stored on many electronic devices will typically be so large that it will often require a search of the device in a law enforcement laboratory or similar facility. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill

three 35' x 35' x 10' rooms to the ceiling. Further, a 500-gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

19. I am also aware that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensics tools. Normally, when a person deletes a file on an electronic device, the data contained in the file does not actually disappear; rather, that data remains until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, *i.e.,* space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

20. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), electronic devices can contain other forms of electronic evidence as well. In particular, records of how an

electronic device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the electronic devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the electronic device was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time

21. Further, evidence of how an electronic device has been used, what it has been used for, and who has used it, may be the absence of particular data on an electronic device. For example, to rebut a claim that the owner of an electronic device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the electronic device remotely is not present on the electronic device. Evidence of the absence of particular

data on an electronic device is not segregable from the electronic device. Analysis of the electronic device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

22. Searching for the evidence described in Attachment B may require a range of data analysis techniques. In some cases, agents and computer analysts may be able to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be co-mingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide information, encode communications to avoid using key words, attempt to delete information to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise to conduct more extensive searches, such as scanning storage areas unrelated to things described in Attachment B, or perusing all stored information briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, the FBI intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

23. Given that the affidavit is in support of a search warrant for electronic devices, which are stored as evidence with the FBI, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

BIOMETRIC ACCESS TO DEVICE(S)

24. This warrant permits law enforcement agents to obtain from the person of the defendant the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any device requiring such

biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the defendant's physical biometric characteristics will unlock the device. The grounds for this request are as follows:

25. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

26. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

27. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be

unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

28. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

29. The passcode or password that would unlock the SUBJECT PHONE subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

30. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped

with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

31. Due to the foregoing, the SUBJECT PHONE may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from the defendant the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock the devices, including to: (1) press or swipe the fingers (including thumbs) of the defendant to the fingerprint scanner of the devices; and/or (2) hold the device in front of the face of the defendant to activate the facial recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.

32. The proposed warrant does not authorize law enforcement to require that the defendant state or otherwise provide the password or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices. Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the defendant to state or otherwise provide that information. However, the voluntary disclosure of such information by the defendant would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask the defendant for the password to the devices, or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks the devices, the agents will not state or otherwise imply that the warrant requires the defendant to provide such information, and will make clear that providing any such information is voluntary and that the defendant is free to refuse the request

FACTS ESTABLISHING PROBABLE CAUSE

33. Since this affidavit is being submitted for the limited purpose of obtaining a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts I believe are necessary to establish probable cause that a search of the SUBJECT PHONE will reveal evidence of the violations of Title 18, United States Code, Sections 922(g)(5)(A)&(B) and 924 (a)(1)(A).

34. I have personally participated in the investigation set forth below. I am familiar with the facts and circumstances of the investigation through my personal participation, from discussions with other investigators, and from my review of records and reports relating to the investigation. The statements in this affidavit are based in part on information received personally during my participation in this investigation as well as information obtained by other law enforcement officers.

35. On February 4, 2018, the defendant was admitted to the United States as a B-2 Visitor which allowed him to remain in the United States until August 3, 2018. The defendant traveled to the United States on an Egyptian passport that was issued on July 25, 2016, with an expiration date of July 24, 2023.[3] The defendant's passport identifies him as an Egyptian national.

36. On August 23, 2018, the defendant completed Form I-589, an Application for Asylum and Withholding of Removal, which was stamped as received by the Department of Homeland Security, U.S. Citizenship and Immigration Services, on August 27, 2018. On October 22, 2018, the defendant was interviewed by an Asylum Officer, and on October 30,

[3] Immigration documents show that on December 3, 2017, the defendant was issued a Type B1/B2 Visa, NIV (Non-Immigrant Visa) #M718345, in Cairo, with an expiration date of November 28, 2022. This Visa permits the defendant to enter the United States but limits his stay to a period of six-moth increments within that time period.

2018, the Asylum Officer denied his Application for Asylum and Withholding of Removal and referred his denial to an Immigration Judge.

37. On November 2, 2018, USCIS issued a Form I-862, Notice to Appear in removal proceedings under section 240 of the Immigration and Nationality Act, also known as the "charging document." The defendant's address on the Notice to Appear was 2391 Fernor Street, Apt. B-18, Allentown, PA 18103, and his area code and phone number was 484-274-9937. The Notice to Appear charges that the defendant had been admitted to the United States, but was removable for the following reasons alleged by the Department of Homeland Security: (1) he was not a citizen or national of the United States; (2) he was a native of Egypt and a citizen of Egypt; (3) he was admitted to the United States at Charlotte, NC on or about February 4, 2018, as a nonimmigrant B-2 with authorization to remain in the United States for a temporary period not to exceed August 3, 2018; and (4) he remained in the United States beyond August 3, 2018, without authorization from the Immigration and Naturalization Service or its successor the Department of Homeland Security. The Notice to Appear states that "[o]n the basis of the foregoing, it is charged that you are subject to removal from the United States pursuant to the following provision(s) of law: Section 237(a)(1)(b) of the Immigration and Nationality Act (Act), as amended, in that after admission as a nonimmigrant under Section 101(a)(15) of the Act, you have remained in the United States for a time longer than permitted." The Notice to Appear requires the defendant to appear before an immigration judge of the United States Department of Justice at 900 Market Street, Philadelphia, PA 19107, on November 28, 2018, at 9:30, to show why he should not be removed from the United States. On November 5, 2018, The defendant signed a Certificate of Service indicating that he was personally served with the Notice

to Appear. The Removal Hearing date was subsequently postponed from November 28, 2018, until April 10, 2019.

38. Accompanying the Notice to Appear, and dated November 5, 2018, was a Referral Notice informing the defendant that USCIS denied his application for asylum after a finding that his claim was not credible. The defendant was informed that his asylum application was referred to an immigration judge for adjudication in removal proceedings. The letter said that "this is not a denial of your asylum application," and that the immigration judge would evaluate his asylum claim independently and was not required to rely on or follow the decision made by USCIS. The Referral Notice also informed the defendant that because he was in removal proceedings, he must notify the Immigration Court within five days of any change of address, and that he was subject to a 150-day waiting period before he could apply for employment authorization, and an additional 30 days before employment authorization could be approved, for a total of 180 days. Because less than 150 days had elapsed since the defendant first filed his asylum application, the Referral Notice stated that he was not eligible to apply for employment authorization until January 24, 2019.

39. On April 10, 2019, the Immigration Court issued a Notice of Hearing in Removal Proceedings to the defendant, 2931 Fernor Street, Apt. B18, Allentown, PA 18103, to appear before the Immigration Court, 900 Market Street, Suite 504, Philadelphia, PA 19107, for a Master/Individual Hearing on May 24, 2022, at 9:00 a.m. The Certificate of Service attached to the Notice indicates that the defendant's attorney was personally served with the Notice on April 10, 2019.

40. On June 20, 2019, the defendant completed an Application for Employment Authorization. In that application, the defendant stated that his immigration status when he

arrived in the United States was as a B-2 visitor. He indicated that his current immigration status was as a B-2 overstay.

41. On July 17, 2019, the defendant was issued an Employment Authorization Card which was valid until July 16, 2021. The card states, "NOT VALID FOR RENTRY TO THE UNITED STATES."

42. On February 5, 2021, the defendant completed another Application for Employment Authorization. In that Application, he stated that his immigration status was as a B-2 visitor, and that his current immigration status was "No Status." [4]

43. On February 26, 2022, the defendant completed a Bureau of Alcohol, Tobacco, Firearms and Explosives, Firearms Transaction Record, Form 4473, to complete the purchase of a Ruger, Model AR556, Serial Number 83996627, rifle, caliber 556, at a gun show in Allentown, PA. The defendant sought to purchase the firearm from a Federal Firearms Licensee ("FFL") that was selling guns at the show. The defendant listed his address on the Form 4473 as 2457

[4] On May 30, 2021, the defendant completed a "Heritage Guild of Easton Range, LLC Customer Information For, Firearms/Archery Experience & Range Safety" form, and a Certification & Release from Liabilities form. On the Customer Information Form, the defendant circled "Yes" to indicate that he was interested in firearms/archery instruction. The defendant listed his address as 2457 30th Street, Allentown, PA 18103, and identified his brother as his emergency contact. A receipt from Heritage Guild of Easton dated May 30, 2021, at 1:30:22 p.m., shows that the defendant purchased ammunition, range rental time, ear and eye protective gear rental, and firearm rental, for $105.46 that was charged to his debit card. The defendant also paid a guest fee for his brother. On June 2, 2021, at 2:03:05 p.m., a receipt from Heritage Guild of Easton shows that the defendant charged a firearm rental, range time, ammunition, and ear and eye protective gear to his debit card in the amount of $65.98. On June 25, 2021, at approximately 1:24:49 p.m., a receipt from Heritage Guild of Easton shows that the defendant charged firearm rental, range time, ammunition, and ear and eye protective gear, for a total amount of $67.04, which the defendant charged to his debit card. On either February 14, 2021, or February 14, 2022 (the form is dated February 14, 2021, but investigation revealed that the correct date may be February 14, 2022), the defendant completed a "Heritage Guild of Easton Range, LLC-Firearms Rental Agreement, on which he stated that he did not meet any of the conditions described in 18 Pa.C.S.A. § 6105(a), (b), and (c), and rented three firearms for target practice . The defendant checked the box on the form that he was participating in the "try before you buy" program. The defendant signed and dated this form. A receipt from Heritage Guild of Easton, dated February 14, 2022, 1:53:12 p.m., shows three firearm rentals, and one long gun rental, ear and eye protection gear rental, a Valentine's Day target, and ammunition, for a total amount of $200.57. A separate receipt on February 14, 2022, 3:07:34 p.m., shows an ammunition purchase in which he exchanged one type of ammunition for another, and a receipt at 3:27:55 p.m., showing that he purchased additional ammunition.

30th Street, Allentown, PA 18103, Lehigh County[5], that his place of birth was Egypt, and he checked the box stating that the United States of America was his country of citizenship. He did not check the box or indicate on the form that Egypt was his country of citizenship. He checked the "no" box to question k which states, "[a]re you an alien illegally or unlawfully in the United States?" He also checked the "no" box to question 21.1.1 which states, "[a]re you an alien who has been admitted to the United States under a nonimmigrant visa?" He left blank both the "yes" and "no" boxes to question 21.1.2 which states, "[i]f you are such an alien do you fall within any of the exceptions stated in the instructions? (U.S. citizens/nationals leave 21.1.2 blank)." He certified that his answers were true, correct, and complete. He signed the Form 4473 on February 26, 2022, after the certification above the signature line, in which the defendant certified that he understands that a person who answers "yes" to 21.1.1, which asks if you are an alien who has been admitted to the United States under a nonimmigrant visa, is prohibited from receiving or possessing a firearm. The certification further stated that making any false oral or written statement or exhibiting any false or misrepresented identification with respect to the transaction, is a crime punishable as a felony under Federal law. A Pennsylvania driver's license was provided as a form of identification, and the defendant's Pennsylvania driver's license number and expiration date are listed on the Form 4473. On February 26, 2022, the FFL submitted the Form 4473 to the NICS (National Instant Background Check System) or the appropriate state agency, PICS (Pennsylvania Instant Background Check System) to complete

[5] A lease obtained from the apartment management company Lehigh Square showed that defendant's brother was the lessee of the apartment at 2457 30th Street, Apt. L-7, Allentown, PA 18103, and that the defendant's brother's move-out date from Apt. L-7 was August 30, 2021. According to Lehigh Square management company, the defendant leased an apartment at 2931 Fernor Street, Apt. B-18, Allentown, PA 18103 beginning February 3, 2018. A lease from the same management company showed that defendant moved from Apt. B-18 to an apartment at 2464 Mountain Lane, Apt. H-23, Allentown, PA 18103, with a lease beginning November 1, 2018, and a move-out date of August 31, 2019. The defendant gave his forwarding address to Lehigh Square as 7032 57th Road, Flushing, New York 11378.

the background check on the defendant regarding the purchase of the Ruger, Model AR556, Serial Number 83996627, rifle, caliber 556. After the gun dealer submitted the Form 4473 completed by the defendant, the NICS/PICS response came back "pending." The defendant waited approximately one hour before the defendant told the gun dealer that he had to leave to pick up his daughter. The defendant gave the gun dealer the SUBJECT PHONE number to contact him when the gun dealer heard from NICS/PIC. The gun dealer wrote the SUBJECT PHONE number on a third page that accompanies the Form 4473.

44. On March 9, 2022, the Honorable Pamela A. Carlos, United States Magistrate Judge, issued a search warrant authorizing cell-site location and pen register information for a cell phone used by the defendant.

45. On March 12, 2022, at approximately 1:00 p.m., I received information from another FBI Special Agent that, pursuant to the cell-site location search warrant signed on March 9, 2022, the cell phone used by the defendant was in the vicinity of a Pennsylvania State Game Land Number 205 Shooting Range located in New Tripoli, Pennsylvania (New Tripoli State Game Land Shooting Range). The FBI Special Agent informed me that he then contacted a Pennsylvania State Game Warden ("Game Warden"), who is also an FBI Task Force Officer ("TFO"), and requested that the TFO Game Warden contact a Game Warden at that location.

46. The TFO Game Warden then contacted the on-duty Game Warden at that location. The TFO Game Warden told the on-duty Game Warden that the TFO Game Warden believed that individuals, including one individual who was not permitted to possess a firearm, were at the New Tripoli State Game Land Shooting Range. I have been informed that it is the responsibility of the on-duty Game Warden to patrol the New Tripoli State Game Land Shooting Range and to check individuals at the location to determine if they have a range permit.

47. While doing patrol on March 12, 2022, the on-duty Game Warden observed the defendant and two other individuals on the shooting range and stopped to inquire if the defendant and the two other individuals had a range permit. As the on-duty Game Warden approached the defendant and the two other individuals[6], the on-duty Game Warden received the information from the TFO Game Warden. The on-duty Game Warden stated that the on-duty Game Warden saw the defendant shooting a firearm while he was on patrol. .

48. In the presence of the on-duty Game Warden and the TFO Game Warden, the defendant stated that the firearm belonged to him. The defendant showed the on-duty Game Warden and the TFO Game Warden a range permit located on the SUBJECT PHONE. The defendant stated that he purchased the rifle from a man he met in an online forum where people from Pennsylvania discussed shooting and firearms. The defendant unlocked the SUBJECT PHONE, and attempted to show the on-duty Game Warden and the TFO Game Warden the forum page. The defendant was unable to open the forum webpage on the SUBJECT PHONE because the webpage would not load.

49. Upon my arrival at the New Tripoli State Game Land Shooting Range with other FBI Special Agents, I observed that the defendant and two other individuals were inside vehicles belonging to the TFO Game Warden and the on-duty Game Warden. Both Game Wardens were standing outside of their vehicles. At this time, the Game Wardens had already confiscated the rifle used by the defendant at the shooting range. The defendant was removed from the vehicle and placed under arrest.

50. The two other individuals with the defendant were identified as his brothers. I interviewed one of the brothers who stated that he and the defendant went to the gun show in

[6] The on-duty Game Warden stated that he approached the defendant after observing him shoot in excess of six rounds in violation of 58 PA Code, § 135.181(b)(6).

Allentown approximately two weeks ago, and that the defendant completed paperwork at the gun show to purchase a firearm. The defendant's brother stated that the gun dealer said either that the system was down or that it was too slow, so the defendant provided the gun dealer with his cell phone number. The defendant's brother stated that the defendant provided the gun dealer with the defendant's telephone number. The defendant's brother said that he did not think that the defendant had heard back from the gun dealer so that the next week, the defendant went to Reading, Pennsylvania to purchase the firearm that he had with him at the New Tripoli State Game Land Shooting Range. The defendant's brother stated that the defendant purchased it with cash from someone in Reading, and that the defendant met the seller on an online forum where people discuss guns and shootings. The defendant told his brother that he received a good deal on it, and that he got a lot of ammunition with it. The defendant's brother also said that he and the defendant went shooting at state game lands last weekend.

51. The firearm possessed by the defendant was identified as a Stag Arms, Model Stag-15, caliber 5.56, bearing serial number 212-915, and a marking stating New Britain, Connecticut, U.S.A. An open source shows that Stag Arms is currently located in Cheyenne, Wyoming, and was previously located in New Britain, Connecticut. Therefore, the firearm possessed by the defendant traveled in interstate commerce.

52. After receiving Miranda warnings and signing a waiver of those rights, the defendant spoke with an FBI SA and the TFO Game Warden. The defendant stated that he was at the gun show in Allentown and that he attempted to purchase a firearm at that time and completed the Form 4473. The defendant stated that on or about March 2, 2022, he purchased a long gun for $1500 in cash at the Airport Diner, Kutztown, PA from a man he believes to be from the Reading, PA area. The defendant was asked for consent to search the SUBJECT

PHONE, but declined consent. The defendant stated that he communicated with the seller of the rifle through an online forum, and that he had the seller's contact information on the SUBJECT PHONE, and that he could retrieve it, but that he would not retrieve it if it granted the FBI SA and the TFO Game Warden access to the SUBJECT PHONE.

CONCLUSION

54. The defendant told the FBI SA and the TFO Game Warden that he had the gun seller's contact information on the SUBJECT PHONE. The defendant also retrieved the range permit to show the on-duty Game Warden from the SUBJECT PHONE. The defendant told the FBI SA and TFO Game Warden that he communicated with the gun seller through an online forum. The defendant also stated that he did not remember the gun seller's name but could retrieve the information from his phone. In addition, the defendant unlocked the SUBJECT PHONE to show the on-duty Game Warden and TFO Game Warden the forum page from the SUBJECT PHONE while at the New Tripoli State Game Land Shooting Range. The defendant also showed the on-duty Game Warden his range permit which was stored on the SUBJECT PHONE. This shows that the defendant uses the SUBJECT PHONE to store information to further his ongoing firearm activities, which violates Title 18, Sections 922(g)(5)(A)&(B) and 924(a)(1)(A). The range permit is relevant to the charged offenses because the range permit is evidence that the defendant intends to possess firearms and ammunition to shoot at a range, and of his motive to provide false information on the Form 4473 to acquire firearms since he cannot acquire them by providing truthful information on the Form 4473.

55. For the reasons set forth above, I respectfully submit that probable cause exists to believe that evidence of violations of Title 18, United States Code, Sections 922(g)(5)(A)&(B) and 924(a)(1)(A) is located on the SUBJECT PHONE, described in Attachment A. I therefore request authorization to search the SUBJECT PHONE seized by investigators from the defendant, and to seize the items from the SUBJECT PHONE described in Attachment B.

/s/ Carmen Dvorak de Morales
Carmen Dvorak de Morales
Special Agent
Federal Bureau of Investigation

SUBSCRIBED AND SWORN TO BEFORE ME
THIS 18th DAY OF MARCH, 2022

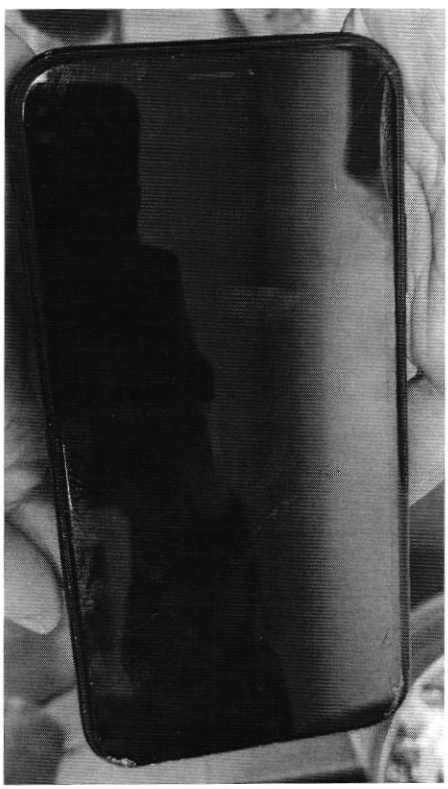
/s/ Richard A. Lloret
HONORABLE RICHARD A. LLORET
United States Magistrate Judge

ATTACHMENT A

ITEMS TO BE SEARCHED

Your affiant is requesting the authorization to search the following item(s):

1. Device 1 is a black colored Apple iPhone; as depicted below:



ATTACHMENT B

Particular Things to be Seized

Evidence of violations of Title 18, United States Code, Sections 924(A)(1)(a) and 922(g)(5)(A) & (B), including the following:

1. All digital images and videos;

2. All records of incoming and outgoing phone calls;

3. All memory, speed dial, and redial features;

4. All voicemails, contact, and address book information;

5. All incoming and outgoing messages and identification information for the senders and recipients, including but not limited to text messages, SMS messages, social-networking messages or alerts;

6. All documents, to include in electronic form, and stored communications, including contact information, text messages, call logs, voicemails, Internet searches, photographs, and any other electronic data or other memory features contained in the devices and SIM cards including correspondence, records, opened or unopened emails, text messages, chat logs, and Internet history, pertaining to the relevant dates described above;

7. All records, documents, invoices, notes and materials that pertain to the ownership or use of the cellular phones;

8. All information and communications concerning the names, addresses, telephone numbers, including any number directory or log stored in the memory of the phone, email addresses, and other contact or identification information of participants involved in the activities described in the above paragraphs;

9. Images, photographs, video recordings, or audio recordings relating to the activities described in the above paragraphs, or depicting the user of the subject phone and any other person involved in or knowledgeable about the activities described in the above paragraphs, or depicting locations at which the above activities occurred or were committed;

10. Location information for the subject phone, including GPS coordinates, location information imbedded in images and videos, map searches, and requests for directions;

11. All deleted files or data;

12. Passwords, encryption keys, and other access devices that may be necessary to access the Subject Phone.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored,

including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

AO 93 (Rev. 11/13) Search and Seizure Warrant (AUSA Mary A. Futcher, requesting)

UNITED STATES DISTRICT COURT

for the
Eastern District of Pennsylvania

In the Matter of the Search of The Cellular Telephone described as a black in color, Apple iPhone, AT&T Mobile Cellular Telephone, with telephone number 484-274-9937	)	Magistrate No. 22-mj-444

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Pennsylvania.
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute the warrant on or before March 29, 2022 *(not to exceed 14 days)*
☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing the warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return the warrant and inventory to the duty magistrate.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing the warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: March 18, 2022 4:11 pm /s/ Richard A. Lloret
Judge's signature

City and state: Philadelphia, PA Honorable Richard A. Lloret, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant left with:
Inventory made in the presence of:		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that the inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title